BAB I

PENDAHULUAN

A. Latar Belakang

Skripsi ini akan mengkaji tentang strategi Privacy International (PI) dalam mengadvokasi isu terkait perlindungan data yang ada di Inggris pada tahun 2017-2020 dengan studi kasus yaitu strategi PI dalam mengadvokasi General Data Protection Regulation (GDPR) milik Uni Eropa. Tujuan dibuatkannya skripsi ini antara lain berguna untuk menganalisis kontribusi yang diberikan oleh Privacy International terhadap perkembangan advokasi isu perlindungan data yang ada di Inggris. Perkembangan teknologi yang begitu pesat terkadang tidak di imbangi dengan dasar hukum yang memadai dalam upaya nya untuk mengatur hingga meminimalisir dampak negatif yang ditimbulkan dari laju perkembangan teknologi tersebut. Salah satu isu yang menjadi perhatian utama terkait privasi pada saat ini yaitu regulasi mengenai perlindungan data. Disinilah peran yang dimainkan oleh Privacy International guna mencegah terulang nya bentuk-bentuk pelanggaran terhadap data individu seperti dalam kasus Cambridge Analytica di tahun 2018 silam melalui perumusan General Data Protection Regulation.

Perlindungan data, terutama menyangkut hak privasi individu sering kali menjadi isu yang diperdebatkan. Perdebatan tersebut pada dasarnya berbicara mengenai *competing values* mulai dari menimbang kebutuhan dalam aspek perlindungan data *(data protection)* dengan tetap memastikan lancarnya alur kebebasan informasi *(free flow of information)*. Selain itu juga terdapat perdebatan terkait bagaimana caranya agar upaya perlindungan privasi individu tidak dikesampingkan ditengah perbincangan mengenai keamanan Nasional. Perdebatan kedua terkait privasi atau keamanan Nasional yang sangat relevan pasca terjadinya 9/11

di Amerika Serikat hingga terkuaknya kasus pengawasan massal NSA ke ranah publik. Setelah kejadian 9/11 tersebut, tingkat perlindungan data terutama di Amerika Serikat dan juga beberapa Negara lainnya mengalami fase kemunduran yang cukup drastis. Upaya perlindungan data yang mana juga membahas tentang hak privasi individu, dikesampingkan dalam beberapa tahun setelahnya dikarenakan urgensi untuk menjaga dan meningkatkan *National security* terutama dari ancaman-ancaman terorisme yang dapat terulang kembali.

Selain karena adanya beberapa *competing values* tersebut, regulasi terkait perlindungan data semakin relevan dikarenakan beberapa alasan, yang pertama yaitu menimbang banyaknya ditemukan kasus-kasus penyelewengan data pribadi mulai dari kasus keterlibatan Facebook dalam kasus Cambridge Analytica ditahun 2018, kebocoran data Equifax tahun 2017, periklanan bertarget, dan masih banyak lagi. Alasan selanjutnya, dikarenakan seiring dengan berjalannya waktu, perkembangan yang amat pesat dibidang teknologi dan informasi terutama melihat dari aspek semakin kompleksnya kegiatan mengumpulkan, memproses, menyimpan dan menggunakan data oleh pihak pengendali sehingga membutuhkan adanya kerangka regulasi ditingkat Nasional dan internasional yang *sufficient* atau memumpuni guna dapat lebih baik mengatur jalannya aktivitas di ruang siber serta memproteksi data pribadi setiap individu dari bentuk-bentuk ancaman baru akibat dari semakin canggihnya kegiatan mengolah data tersebut.

Ketika berbicara mengenai perlindungan data, maka salah satu ancaman yang dihadapi yaitu terkait fenomena *data breach* atau kebocoran data dimana kasus kebocoran data seringkali ditemukan dalam sepuluh tahun belakangan ini dan kejadian tersebut dapat merugikan korban baik dari segi materil maupun non-materil. Beberapa kasus besar melibatkan segilintir perusahaan ternama seperti dalam kasus Equifax (2017), Cambridge Analytica (2018) dan Tokopedia (2020) di Indonesia. Menurut lembaga National Cyber Security Centre di Inggris (UK NCSC), kasus kebocoran data terjadi ketika

informasi yang dipegang oleh suatu organisasi dicuri atau diakses oleh pihak ketiga tanpa izin dari pihak yang berwenang atau pihak yang memiliki otoritas atas data tersebut. Kejadian ini tentunya berdampak secara negatif dan umumnya melibatkan konsumer sebanyak puluhan hingga ratusan juta orang dimana data pribadi mereka tereskpos dan dalam beberapa kasus diperjual belikan secara illegal melalui *dark web*. Dikarenakan aktivitas mengumpulkan, memproses hingga menggunakan data pribadi individu berlangsung tidak hanya disatu sektor saja, namun di hampir berbagai sektor, seperti contoh disektor kesehatan, perbankan dan industri IT, maka biasanya insiden *data breach* terjadi karena pihak ketiga sedari awal telah mengincar suatu organisasi dari sektor tertentu dengan maksud dan tujuan yang spesifik.

Bentuk informasi seperti apa yang ingin di ekstraksi dari pembobolan data tersebut juga berbeda tergantung pada sektor yang dijalani dari tiap-tiap organisasi. Selain data pribadi individu yang umumnya terdiri dari nama, alamat IP, alamat tempat tinggal, kata sandi ataupun tanggal lahir seseorang, data-data yang dikumpulkan dan diproses oleh sektor tertentu seperti perbankan yang memiliki *database* terkait tenggat waktu kartu kredit seseorang dan nomor rekening dari seluruh nasabahnya pun ikut menjadi target dari fenomena kebocoran data. Hal ini serupa dengan alasan terjadinya kebocoran data dibeberapa sektor lainnya dimana organisasi/perusahaan menyimpan informasi tertentu mulai dari sektor IT, organisasi yang bergelut dalam bidang hak cipta, maupun disektor kesehatan yang seperti contoh menyimpan informasi mengenai kondisi kesehatan suatu pasien, resep obat yang diberikan oleh Dokter hingga informasi mengenai rekam medis seseorang. Lebih lengkapnya, untuk pembahasan terkait beberapa contoh kasus kebocoran data yang telah terjadi, besarnya jumlah individu yang data pribadi nya bocor akibat dari suatu kasus serta dampak yang ditimbulkan dapat dipahami sebagai berikut.

Contoh kasus kebocoran data dengan skala yang masif terjadi pada tahun 2017 dimana Equifax, salah satu perusahaan

Credit Reference Agencies (CRAs) terbesar dari Amerika Serikat mengalami kebocoran data dan berakibat pada terekspos nya informasi pribadi dari sekitar 148 juta konsumen nya. Walaupun mayoritas individu yang terdampak berasal dari AS, namun data pribadi dari beberapa warga Inggris (693,665) pun ikut terekspos dalam kasus tersebut. Bentuk data pribadi yang bocor pun sifatnya sensitif, mulai dari informasi mengenai Social Security Numbers (SSN), nomor lisensi mengemudi, alamat email dan informasi kartu kredit dari para konsumen nya. Kasus ini mendapatkan perhatian baik dari pemerintah di tingkat lokal, Negara bagian maupun Federal AS hingga di Inggris. Untuk penanganan kasus Equifax di Inggris, UK Financial Conduct Authority merupakan badan yang memiliki wewenang dalam memberikan denda kepada perusahaan terkait dan menarik izin Equifax untuk menjalankan aktivitas pengecekan kredit di Inggris. Sementara perihal investigasi lebih lanjut dilakukan oleh Information Commissioner's Office (ICO)—selaku badan otoritas perlindungan data di Inggris. Pasca kebocoran data tersebut terjadi, dalam beberapa kasus lainnya biasanya data-data yang terekspos tidak lama kemudian akan muncul di *dark web* untuk diperjual belikan secara illegal. Namun, dalam kasus Equifax, pihak penyelidik tidak menemukan adanya satu pun data pribadi yang dijual melalui *dark web* bahkan setelah pihak penyelidik menunggu cukup lama. Hal ini membuat tanda tanya besar, terkait untuk apa data dengan jumlah cangkupan yang massif tersebut kemudian digunakan selanjutnya, siapa dan untuk tujuan apa kebocoran data tersebut terjadi.

Kasus selanjutnya yaitu Cambridge Analytica di tahun 2018 yang mana merupakan salah satu bentuk contoh kasus kebocoran data yang mendapatkan atensi dan kritik cukup intens dari publik. Kasus ini melibatkan salah satu perusahaan IT raksasa dari Silicon Valley yaitu Facebook dimana data pribadi dari sekitar 87 juta pengguna platform tersebut terekspos dan digunakan oleh Cambridge Analytica, sebuah firma *consulting politic* sekaligus perusahaan *data broker* dari Inggris dalam Pemilihan Umum Presiden Amerika Serikat

tahun 2016 silam (Gross, 2019). CA merupakan anak perusahaan dari SCL yang fokus beroperasi dalam bidang *data mining, analysis*, dan *data brokerage*. Terkuaknya kasus ini bermula ketika seorang *whistle blower* dari Cambridge Analytica (CA), yaitu Christopher Wylie mengekspos kasus tersebut kepada wartawan dari The Guardian. Kasus ini memiliki dampak yang signifikan terutama mengingat bahwa data pribadi individu yang dipanen oleh CA melalui platform Facebook selanjutnya digunakan untuk kepentingan politik, tepatnya dalam aktivitas kampanye kandidat Presiden dari partai Republik yaitu Donald Trump pada Pemilu tahun 2016 silam. Data-data pribadi pengguna Facebook dikumpulkan, diolah dan digunakan oleh CA tanpa sebelumnya mendapatkan izin maupun konsen dari pemilik data tersebut yang mana melanggar prinsip-prinsip perlindungan data dan tentunya hak privasi individu. Data yang telah diolah tersebut kemudian digunakan dalam *microtargeting*—sebuah metode yang sering digunakan dalam kampanye politik dan dilakukan secara online.

Melalui kedua contoh kasus kebocoran data yang telah dijabarkan sebelumnya, yaitu kasus Equifax di tahun 2017 dan Cambridge Analytica di tahun 2018, dapat dilihat bahwa terdapat beberapa ancaman nyata serta dampak negatif yang ditimbulkan akibat dari adanya kebocoran data. Kasus Equifax merupakan contoh kasus kebocoran data di sektor perbankan dimana data yang bocor tersebut melibatkan hampir setengah dari warga Negara Amerika Serikat. Data-data yang sifatnya sensitif tersebut dapat jatuh ke tangan *cybercriminal* yang biasanya berujung kepada pencurian identitas *(identity theft)* dan dimanfaatkan untuk beberapa tindak kriminal lainnya seperti *phising* dan *tax fraud*. Tindak kriminal tersebut merupakan beberapa skenario yang dapat terjadi pada kejadian kebocoran data pada umumnya. Namun, dalam kasus Equifax, kesimpulan yang didapat yaitu data-data pribadi yang sifatnya sensitif dan mencangkup banyak warga Negara di AS tersebut merupakan bentuk espionase dari Pemerintah Republik Rakyat Tiongkok terhadap Amerika Serikat. Sementara dalam kasus

Cambridge Analytica di awal tahun 2018 memperlihatkan bentuk dampak dari kebocoran data berupa data-data yang didapatkan tanpa adanya konsen dari individu terkait digunakan oleh pihak ketiga yaitu CA dalam Kampanye Politik ketika Pemilihan Umum Presiden AS tahun 2016 maupun dalam kampanye *Vote Leave Brexit* di Inggris. Data-data tersebut dimanfaatkan melalui metode *microtargeting* dimana pesan dari kampanye politik sifatnya lebih difokuskan ke masing-masing individu bukan umum.

Kasus Cambridge Analytica memperlihatkan contoh penyelewengan penggunaan data dari platform media sosial untuk kepentingan politik dari suatu kelompok, mengindikasikan adanya bentuk pelanggaran HAM, terutama menyangkut hak atas privasi dari masing-masing individu. Salah satu kritik yang muncul akibat kasus CA yaitu ketika para pengguna platform sosial media dan jasa IT ini tidak lagi berperan sebagai *customer* dari perusahaan mereka, namun sekaligus menjadi obyek komoditas yang di perjual-belikan tanpa persetujuan dari para pengguna nya. Model bisnis yang memiliki celah keamanan tersebut tidak hanya terbatas di lingkup media sosial saja, namun juga dibeberapa platform yang memiliki fungsi untuk mengumpulkan, menyimpan, memproses dan menggunakan data pribadi dari para pengguna jasa mereka.

Platform media sosial menawarkan dan menyediakan aplikasi mereka untuk digunakan secara gratis oleh masyarakat, dengan konsekuensi atau timbal balik yaitu data berisi informasi pribadi dari konsumen dapat disimpan, dikumpulkan dan digunakan oleh perusahaan tersebut. Model bisnis seperti inilah yang diaplikasikan oleh sejumlah besar perusahaan IT (Amnesty International, 2019). Setelah perusahaan tersebut berhasil menyimpan data pribadi dari para pengguna platform milik-nya, data tersebut kemudian akan dianalisis dan dikategorisasi kedalam sub-sub data yang memudahkan perusahaan untuk melihat pola ketertarikan, karakteristik, serta tingkah laku dari para penggunanya (Karunian & Halme, 2019).

Tujuan akhir dari proses ini yaitu menciptakan profit dari penjualan iklan yang tepat sasaran melalui *insight* data yang telah mereka olah sebelumnya. Kemampuan inilah yang terkadang digunakan secara tidak etis dengan cara menyelewengkan data dari para pengguna platform, tanpa sepengetahuan dari para pemilik data tersebut.

Privacy International atau PI merupakan NGO yang memiliki tujuan untuk mengubah dan mencegah terulangnya kembali hal-hal negatif dalam isu perlindungan data seperti yang telah dijabarkan sebelumnya. Fokus target dari advokasi PI lebih menargetkan kepada dua aktor, yaitu model bisnis organisasi yang menyimpan data-data pribadi individu dari konsumennya maupun Pemerintah terutama dalam hal aktivitas pengawasan massal. PI merupakan NGO dari Inggris, namun begitu, advokasi yang dilakukan mencangkup wilayah bahkan diluar Eropa seperti di Asia, Timur Tengah, Amerika Latin, dsb. Advokasi yang dilakukan pun membahas tentang perlindungan data diberbagai sektor, mulai dari kampanye tentang hubungan antara utilisasi data dengan kampanye politik (Amerika Latin), alat transparansi yang digunakan dalam *political advertising* oleh Facebook dan Google, penjelasan terkait bentuk-bentuk resiko yang muncul akibat dari penggunaan sistem *profiling* pada visa melalui kebijakan *travel initiative* yang diberlakukan oleh Uni Eropa serta pembuatan *draft* Perlindungan Data Pribadi (PDP) di Indonesia.

Maka dari itu, penelitian ini akan fokus pada strategi Privacy International (PI) dalam mengadvokasi isu terkait perlindungan data yang ada di Inggris pada tahun 2017-2020 dengan studi kasus yaitu advokasi PI dalam perumusan General Data Protection Regulation milik Uni Eropa.

B. Rumusan Masalah

Mengacu kepada latar belakang yang telah disebutkan diatas, maka rumusan masalah yang dapat diajukan yaitu: Bagaimana strategi *Privacy*

International dalam mengadvokasi isu perlindungan data di Inggris melalui GDPR pada tahun 2017-2020?

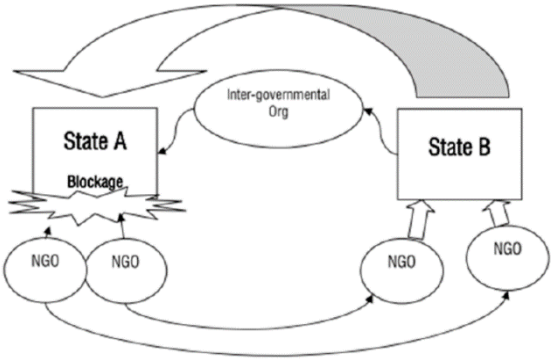
C. Kerangka Pemikiran

Model Transnational Advocacy Network (TAN)

Penerapan dari *Transnational Advocacy Network* (TAN) atau Jejaring Advokasi Internasional milik Margaret E. Keck dan Kathryn Sikkink seringkali ditemukan dalam strategi yang ditempuh oleh beberapa LSM dan juga IGO *(International Governmental Organisation)*, seperti UNHCR, Greenpeace dan Amnesty International. Namun, dalam penelitian kali ini, fokus dari penerapan model TAN akan diaplikasikan pada LSM Privacy International. Model ini menggambarkan hubungan koordinasi antar aktor advokasi lintas Negara dengan tujuan untuk mempengaruhi hingga mengubah arah kebijakan atau kondisi yang ada pada suatu Negara agar sesuai dengan yang dikehendaki dari para aktor advokasi tersebut. Bentuk kerja sama dapat terjalin karena adanya kesamaan isu yang ingin diperjuangkan antar satu aktor dengan aktor advokasi lainnya. Seperti contoh yaitu kesamaan isu mengenai krisis pengungsi, lingkungan, kesetaraan gender, dsb. Aktor advokasi transnasional yang dimaksudkan oleh baik Keck dan Sikkink disini mencangkup beberapa pihak seperti dari kalangan kelompok LSM yang sifatnya domestik maupun internasional, media massa, serikat buruh, para kelompok cendikiawan, *Inter-governmental Organisation* (IGO) maupun dari pemerintahan lokal.

Terkait alur koordinasi para aktor advokasi tersebut, Keck dan Sikkink lebih lanjut memperkenalkan model dari *Boomerang Pattern*. *Boomerang Pattern* menjelaskan mengenai pola komunikasi antar aktor advokasi lintas Negara yang saling berkoordinir dalam rangka mengarahkan serta mempengaruhi hasil kebijakan yang ada pada suatu Negara melalui desakan-desakan atau *international pressure* yang datang dari Negara lain serta *Inter-governmental Organisation* (IGO). Tahapan ini ditempuh karena pertama-tama adanya hambatan atau blokade yang dilakukan oleh pemerintah terhadap LSM-LSM domestik. Maka dari itu, cara alternatif bagi NGO dalam mengubah kebijakan Negara yang telah memblokade usaha mereka yaitu melalui komunikasi dan kerja sama dengan NGO yang berada di Negara lain. Untuk lebih jelasnya, dapat dilihat ilustrasi model *Boomerang Pattern* berikut.

Gambar 1.1 Model *Boomerang Pattern*



Sumber : Keck & Sikkink, Activists Beyond Border: Advocacy Networks in International Politics (1998), hal. 13 (Margaret E. Keck, 1988).

Strategi yang diusung dalam TAN dapat dibagi kedalam empat kelompok besar atau tipologi, yaitu: *information politics, symbolic politics, leverage politics,* dan *accountability politics.* Yang pertama, *Information Politics* adalah kemampuan untuk mentransfer informasi politik yang kredibel secara cepat dan tepat ke tempat dimana informasi tersebut dapat digunakan untuk membuat dampak perubahan yang signifikan. Kedua, *Symbolic Politics* membahas tentang kemampuan anggota jaringan untuk menggunakan bentuk-bentuk simbol, tindakan, hingga cerita yang dapat menggambarkan isu yang ingin dibawa kepada masyarakat umum. Selanjutnya, *Leverage Politics* yaitu kemampuan dalam mengarahkan aktor-aktor dengan kekuatan dan posisi penting untuk mempengaruhi masyarakat luas. Sementara strategi terakhir yaitu *Accountability Politics* membahas tentang kemampuan anggota jaringan dalam menjaga dan mengawasi pemerintah untuk tetap mempertahankan kebijakan-kebijakan yang telah sesuai dengan tujuan mereka.

Berangkat dari gabungan penjabaran mengenai empat tipologi strategi jaringan advokasi milik Keck dan Sikkink dan konsep Hak Privasi Individu, aplikasi dari model TAN dalam kasus strategi yang digunakan oleh Privacy International dalam mengadvokasi isu hak privasi data di Inggris dapat dipahami sebagai berikut:

1. Information Politics

Privacy International mengartikulasikan strategi *Information Politics* dengan cara menekankan bahwa isu perlindungan data tidak lepas kaitannya dengan HAM seseorang, terutama

dengan hak privasi individu. PI pun menyadari pentingnya untuk memanfaatkan kehadiran internet sebagai alat dalam menyebarkan informasi terkait perlindungan data kepada publik secara lebih efektif. Maka dari itu, advokasi gencar dilaksanakan secara daring dengan bentuk informasi yang beragam, mulai dari teks, info statistik, ilustrasi ataupun video sehingga memudahkan masyarakat dalam mengakses informasi tersebut. PI dalam upaya nya untuk membuat dampak perubahan yang signifikan terhadap perlindungan data di Inggris, ikut bekerja sama dengan beberapa media massa lokal dan internasional, seperti yang ditunjukkan melalui peran yang dimainkan oleh PI dalam proses perumusan *General Data Protection Regulation* (GDPR) oleh Uni Eropa dengan cara memperbaharui informasi pada laman website dan beberapa *platform* media sosial yang mereka miliki terkait perkembangan perumusan hingga bentuk implementasi dari GDPR (Privacy International, 2019).

Hal ini dilakukan dengan maksud menyebarluaskan informasi terkait bentuk kebijakan perlindungan data seperti apa yang harus diambil oleh Pemerintah Inggris, tentunya dengan lingkup audiens yang lebih luas pula. Bentuk-bentuk pemberitaan yang dilakukan tersebut bertujuan agar dampak dari advokasi yang dilakukan oleh Privacy International dapat secara luas diakses dan diterima oleh masyarakat tanpa memandang keterbatasan geografis ataupun kondisi finansial mereka.

2. Symbolic Politics

Symbolic politics merupakan strategi kedua yang terdapat dalam TAN. Strategi ini pada

dasarnya membahas tentang kemampuan jaringan dalam menggunakan simbol, tindakan atau narasi untuk membenarkan isu yang ingin diangkat dan juga bertujuan dalam mempengaruhi pandangan publik terhadap isu tertentu. Penerapan dari strategi *Symbolic Politics* oleh Privacy International ditunjukkan melalui serangkaian aktivitas kampanye baik yang secara langsung maupun tidak langsung terkait GDPR dan perlindungan data secara runtut dan komprehensif, serta menjalin kerja sama dengan beberapa NGO lainnya dalam berkampanye. Selain dari kampanye, PI ikut merayakan Hari Perlindungan Data Internasional yang diperingati pada tanggal 28 Januari tiap tahun nya (Privacy International, Data Protection Day 2018: A Global Perspective to Privacy, 2019). Hal ini sejalan dengan tulisan dari Margaret E. Keck dan Kathryn Sikkink yang menjelaskan perihal aktor-aktor advokat yang berupaya dalam aktivitas *framing* atau membingkai masalah dengan mengidentifikasi dan memberikan penjelasan yang meyakinkan dalam kumpulan peristiwa-peristiwa simbolik yang kuat, yang pada akhirnya akan membawa perubahan terhadap pola pikir serta tindakan dari masyarakat maupun pihak pembuat kebijakan.

3. Leverage Politics

Leverage Politics dapat dimaknai sebagai sebuah kemampuan NGO dalam mengarahkan aktor-aktor yang menduduki posisi penting dan memiliki kekuatan lebih besar dari NGO tersebut untuk mempengaruhi masyarakat luas terhadap suatu isu. Strategi ini pada dasarnya membahas mengenai kemampuan Privacy International dalam mengarahkan aktor-aktor dengan kekuatan dan posisi penting untuk mempengaruhi masyarakat luas terkait perlindungan data. Hal ini ditunjukkan

seperti contoh dalam tahapan awal advokasi GDPR, dimana PI menggandeng beberapa aktor baik IGO maupun LSM-LSM domestik dan internasional yang memiliki pengaruh lebih dalam membantu proses advokasi perlindungan data. Contoh aktor-aktor tersebut yaitu Uni Eropa, Komisioner Tinggi HAM PBB, hingga koalisi yang saat itu terbentuk khusus untuk membantu Uni Eropa dalam perumusan draft awal GDPR. Koalisi tersebut merupakan gabungan dari beberapa NGO yang berasal dari luar Inggris seperti European Digital Rights (EDRi) dari Belgium, Digitale Gesellschaft dari Jerman, Digital Rights Ireland dan Bits of Freedom dari Belanda. Selain dari koalisi yang tercipta di tahap awal perumusan GDPR, dalam perkembangannya Privacy International juga bekerja sama dengan NGO yang bergerak dibidang HAM dan masih berasal dari Inggris seperti contoh Liberty dan Open Rights.

4. Accountability Politics

Strategi akhir yang ditempuh oleh Privacy International sebagai sebuah organisasi yaitu *Accountability Politics*. *Accountability Politics* merupakan upaya yang dilakukan oleh jaringan dalam menekan aktor-aktor berpengaruh lainnya untuk bertindak sesuai dengan kebijakan atau nilai-nilai yang sebelumnya telah diperkenalkan, disetujui dan didukung secara formal oleh aktor tersebut. Strategi ini diterapkan oleh Privacy International dengan cara mengawasi pemerintah Inggris dalam menjalankan dan menegakkan GDPR yang telah diadopsi di Inggris sesuai dengan yang telah diatur dalam *United Kingdom Data Protection Act* 2018 (UK DPA 2018).

D. Hipotesa

Privacy International menggunakan serangkaian strategi sesuai dengan yang terdapat pada empat tipologi TAN dikarenakan sebagai sebuah aktor NGO, usaha dalam mempengaruhi arah kebijakan Inggris terkait perlindungan data tidak cukup hanya bekerja secara mandiri saja tetapi juga memerlukan dukungan serta kerja sama dari aktor-aktor berpengaruh lainnya.

E. Metode Penelitian

1. Metode Analisis Data

Peneliti akan menggunakan metode analisis data kualitatif yang bersifat deskriptif. Data yang telah diperoleh selanjutnya akan dikelola, diorganisasikan dan kemudian menyusun hasil yang telah diputuskan. Bersifat deskriptif karena akan menjelaskan proses terjadinya suatu peristiwa.

2. Teknik Pengumpulan Data

Teknik yang digunakan dalam penelitian ini adalah dengan mengumpulkan berbagai sumber seperti dari berbagai literatur yang berhubungan dengan penelitian baik berupa buku, jurnal ilmiah, surat kabar, hasil diskusi ilmiah, laporan media, dan data dari website resmi organisasi internasional, LSM serta pemerintah yang terkait.

F. Jangkauan Penelitian

Penelitian ini akan terfokus kepada strategi yang ditempuh oleh Privacy International dalam upaya-nya untuk mengadvokasi isu perlindungan data di Inggris melalui GDPR dalam kurun waktu tiga tahun, yaitu dari tahun 2017 hingga 2020.

G. Sistematika Penulisan

Struktur penulisan dari skripsi ini terdiri atas tiga bab, yaitu:

BAB I : PENDAHULUAN

Pada bab pendahuluan dijelaskan secara singkat terkait latar belakang masalah serta terdiri atas rumusan masalah, kerangka pemikiran yang digunakan dalam menganalisis studi kasus, hipotesa, metode penelitian hingga jangkauan penelitian.

BAB II : PERKEMBANGAN REGULASI PERLINDUNGAN DATA DAN IMPLEMENTASI GENERAL DATA PROTECTION REGULATION DI INGGRIS

Pada bab ini akan dijelaskan mengenai beberapa hal mulai dari sejarah hingga kondisi dari kerangka regulasi perlindungan data ditingkat global yang berlaku saat ini maupun beberapa permasalahan yang seringkali muncul dan menjadi tantangan dalam upaya meningkatkan perlindungan data. Pembahasan selanjutnya akan mencangkup lebih rinci terkait regulasi General Data Protection Regulation (GDPR) hingga implementasi nya di Inggris.

BAB III : PERAN PRIVACY INTERNATIONAL DALAM MENGADVOKASI ISU PERLINDUNGAN DATA DI INGGRIS MELALUI GENERAL DATA PROTECTION REGULATION

Bab ini akan dibuka dengan penjelasan mengenai isi dari General Data Protection Regulation dan implementasi-nya di Inggris. Kemudian dilanjutkan dengan analisis peran

Privacy International dengan menggunakan empat tipologi yang terdapat dalam TAN (*Transational Advocacy Network)* milik Keck & Sikkink.

BAB IV : KESIMPULAN

Pada bab kesimpulan ini berisi kesimpulan dari keseluruhan bab.